TLP:WHITE

CISA Region I (RHODE ISLAND)

Cybersecurity Advisor Program

MIKE (ROLAND) TETREAULT
Cybersecurity Advisor, Region I (RI)
Cybersecurity and Infrastructure Security Agency (CISA)
Cell: 202-941-1288
EMAIL: Roland.Tetreault@cisa.dhs.gov

Cybersecurity Advisor Program

TLP:WHITE

CISA mission: Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure

In support of that mission: Cybersecurity Advisors (CSAs):

- **Assess**: Evaluate critical infrastructure cyber risk.
- **Promote**: Encourage best practices and risk mitigation strategies.
- **Build**: Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Inform and raise awareness.
- **Listen**: Collect stakeholder requirements.
- **Coordinate**: Bring together incident support and lessons learned.

CISA CYBER+INFRASTRUCTURE

Misconceptions Vs. Reality

TLP:WHITE

Common Misconceptions

- You need a big budget!
- Silver Bullet!
- Why would we be a target?
- There's too much to do!
- We don't own the risk!

Reality

- Step-by-step process: Crawl-Walk-Run
- Get the "101" stuff in order
- A good asset inventory
- Research the solutions!
- You do own the risk!

CISA
CYBER+INFRASTRUCTURE

3 Items to Take Away

TLP:WHITE

1. Ransomware, Information Stealers, and Banking Trojans are still the most likely threat to organizations typically originating as Phishing activity. ***Cyber Awareness Training is where this defense starts!***

---

2. Continue to focus your efforts around building a Cyber Hygiene organizational culture first then ***build detection and response capacity to identify and contain known malicious activity quickly.***

---

3. ***Public and Private partnerships absolutely make a difference.*** We have come a long way when it comes to threat information sharing across the cybersecurity community and it is absolutely making a difference in our ability to respond and deter the threat actor. CISA values partnerships and is counting on a community approach to better protect and safeguard the homeland.

Visit **CISA.gov/ransomware** for more information.

CISA
CYBER+INFRASTRUCTURE

CISA Cybersecurity Offerings

TLP:WHITE

Local CSA Provided

- **Preparedness Activities**
  - Information/Threat Indicator Sharing
  - Cybersecurity Training and Awareness
  - Cyber Exercises and “Playbooks”
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices / MS-ISAC – EI-ISAC
  - **Cybersecurity Service Offerings**
    - Cyber Resilience Reviews (**CRR**)
    - External Dependency Management (**EDM**)
    - Cyber Infrastructure Surveys (**C-IST**)
    - Cyber Security Evaluation Tool (**CSET**)

CISA HQ Response Assistance

- Remote / On-Site Assistance
- Malware Analysis
- Hunt and Incident Response Teams
- Incident Coordination

Cybersecurity Advisors (CSA)

- Assessments
- Working group collaboration
- Resiliency Workshops
- Best Practices private-public
- Incident assistance coordination

Protective Security Advisors

- Physical Security Assessments
- Incident liaisons between government and private sector for CI protection
- Support for National Special Security Events

Delivered by CISA Vulnerability Mgt Team

- Phishing Campaign Assessment (PCA)
- Cyber Hygiene Scanning (CyHy)
- Web Application Scanning (WAS)
- Remote Penetration Testing (RPT)
- Risk & Vulnerability Assessment (RVA)
- Red Team Assessment (RTA)
- Validated Architecture Design (VADR)
- Critical Product Evaluation (CPE)
- CISA Qualification Initiative (CQI)

CISA CYBER+INFRASTRUCTURE

What Is a Cyber Resilience Review

THE CRR IS…	THE CRR IS NOT…
An assessment of an organization's practices that support the management of cybersecurity risk	Meant to make a value judgement on an organization's cyber resilience
A review of an organization's mission-critical service	An examination of an organization's IT and business operations
A facilitated, interview-based review	A technical assessment, i.e., no technical probing, scanning, or testing of networks or systems
A capability-based review of cybersecurity management practices	A control-based audit of an organization's cybersecurity posture
Meant to measure the level of process institutionalization	Meant to measure the effectiveness of implemented cybersecurity controls
Meant to start a constructive dialogue for improving cybersecurity management	To be used for regulatory purposes

CISA
CYBER+INFRASTRUCTURE

CRR Domains

AM	Asset Management
CM	Controls Management
CCM	Configuration and Change Management
VM	Vulnerability Management
IM	Incident Management
SCM	Service Continuity Management
RM	Risk Management
EDM	External Dependencies Management
TA	Training and Awareness
SA	Situational Awareness

CISA
CYBER+INFRASTRUCTURE

Cyber Resilience Reviews (CRR)

TLP:WHITE

Cybersecurity Management

- Leadership
- Inventory
- System Architecture
- Change Management
- Lifecycle Tracking
- Assessment & Evaluation
- Cybersecurity Plan
- Information Sharing

Incident Response

- Incident Response Measures
- Alternate Site & Disaster Recovery

Cybersecurity Controls

- Access Controls
- Access Paths
- Malicious Code Controls
- Monitor & Scanning
- User Training

Dependencies

- Data at Rest
- Data in Motion
- Data in Process
- Endpoint Systems

CISA
CYBER+INFRASTRUCTURE